


DEPARTMENT OF PERSONNEL & ADMINISTRATION		HIPAA Policy No.	6
		Current Effective Date	April 12, 2007
		Original Effective Date	May 1, 2006
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT		Approved by: David M. Kaye	
SYSTEM ACCESS (ACCESS TO EPHI)		Date: <i>4/16/07</i>	

I. Purpose

To ensure the confidentiality, integrity, and availability of electronic protected health information ("ePHI") created, received, maintained or transmitted by the Department of Personnel and Administration ("DPA").

II. Policy

It is DPA's policy to control and limit access to all protected health information ("PHI"). Only those employees or groups of employees who have been described in plan documents are authorized to use or disclose PHI. Access to electronic protected health information (ePHI), which is the focus of this policy, is further limited to the subset of employees or groups of employees identified in this policy.

Employee's may use their access privileges only to perform assigned job functions requiring the use of ePHI. When using ePHI, an employee must limit use to the minimum amount necessary to carry out the specific task at hand. Any employee who unnecessarily accesses ePHI, who accesses more ePHI than necessary, or who allows another individual access to ePHI, will be subject to sanctions in accordance with DPA's HIPAA Sanctions policy.

Access will be terminated upon termination of employment, or upon a change of job or job functions that eliminates the need for access to ePHI.

A. Employees Authorized for Access

1. The following DPA employees or groups of employees are permitted to use or access ePHI, provided they do so in accordance with HIPAA regulations and DPA and DHR policies and procedures.
 - a. **Employee Benefits Unit (EBU)** restricted to those functions and activities performed on behalf of the state employees group benefit plans.
 - b. **Colorado State Employee Assistance Program (CSEAP)** restricted to the operations of CSEAP, including use of the CSEAP tracking application.
 - c. **DHR's Total Compensation Strategist** restricted to those functions and activities performed on behalf of the state employees group benefit plans.
 - d. **DHR's Total Compensation Statistical Analyst** restricted to those functions and activities performed on behalf of the state employees group benefit plans.
 - e. **DPA's HIPAA Compliance Officer** limited to ensuring and enforcing compliance with HIPAA regulations.

- f. **DPA's Chief Information Officer (CIO)** limited to performing services for or related to state employees group benefit plans.
 - g. **Information Technology Unit (ITU)** limited to the services it performs for or related to state employees group benefit plans that would make ITU a business associate if it were a separate legal entity.
 - h. **Technology Management Unit (TMU)** limited to the services it performs for or related to state employees group benefit plans that would make TMU a business associate if it were a separate legal entity.
 - i. **Information Security Operations Center (ISOC)** limited to the services it performs for or related to state employees group benefit plans that would make ISOC a business associate if it were a separate legal entity.
 - j. **Server Team** limited to the services it performs for or related to state employees group benefit plans that would make the Server Team a business associate if it were a separate legal entity.
2. IT employees (ITU, TMU, ISOC, and Server Team) shall be given access only on an as needed basis and only to the extent necessary to carry out the responsibilities of their positions that relate to EBU and CSEAP electronic data. Access must be authorized by the CIO or delegate.
 3. Other authorized users of PHI who believe they have a need for PHI maintained in electronic form must contact one of the following individuals, in the order listed, based upon availability. The individual contacted will review the request and the ePHI, and determine what, if any information from the ePHI shall be given to the requestor. The requestor will not have direct access to the system containing ePHI.
 - For EBU data
 - ◆ EBU Program Supervisor
 - ◆ Contract Administrator of the health plan involved
 - ◆ DPA's HIPAA Compliance Officer
 - For C-SEAP data^{*}
 - ◆ C-SEAP Program Supervisor
 - ◆ DPA's HIPAA Compliance Officer
 - ◆ C-SEAP Office Manager

B. Modification or Termination of Access

1. An employee's access must be terminated upon termination of employment, a change of job or job function that eliminates the need for access, or if there is evidence or reason to believe any of the following:
 - the employee is using (or has used) access rights inappropriately;
 - an employee's log-in or password has been compromised (a new log-in or password may be provided if the employee is not identified as the one compromising the original log-in or password); or
 - someone is using (or has used) another individual's log-in and password (a new log-in and password may be provided if the employee is not identified as the one providing someone else with the log-in and/or password).

^{*} Disclosure of C-SEAP information is further restricted by State law.

2. The access privileges of an employee on disciplinary action may be suspended, modified, or terminated at the discretion of the appointing authority.
3. The access privileges of an employee on leave of absence may be suspended or terminated at the discretion of the appointing authority.

C. Review of Access Privileges

Access privileges shall be reviewed:

- each time an employee's job or job functions change;
- when an employee is placed on disciplinary action;
- when an employee takes an extended leave of absence;
- by DPA's HIPAA Compliance Officer as part of the programs for monitoring and auditing HIPAA compliance;
- by appropriate ITU, TMU, ISOC, or Server Team personnel as part of the access control function.

D. Responsibilities of Employees with Access to ePHI

1. Passwords must be protected in accordance with DPA's policy on Password Management.
2. Logins must be protected.
3. Employees must never allow anyone not expressly authorized to access ePHI to access or view ePHI.
4. Screensavers on systems containing ePHI or through which ePHI can be accessed must be turned on, password-protected, and set to activate after fifteen (15) minutes of inactivity.
5. Employees must log out of a program containing or accessing ePHI as soon as they are finished using the program.
6. Employees must lock their computer system, or log out of a program containing or accessing ePHI, when they leave their workstations.

III. Procedures

Procedures consistent with this policy for granting, modifying, and terminating access to ePHI shall be developed under the supervision of the CIO, with input from DPA's HIPAA Compliance Officer.

IV. Definitions/Abbreviations

None

V. Revision History

<u>Date</u>	<u>Description</u>
May 1, 2006	Original document
March 26, 2007	Revised to be consistent with HIPAA Policy 1, Organizational Designations

VI. References/Citations

45 CFR 164.308(a)(3)(ii)(A)	Authorization and/or Supervision
45 CFR 164.308(a)(3)(ii)(C)	Termination Procedures
45 CFR 164.308(a)(4)(ii)(B)	Access Authorization
45 CFR 164.308(a)(4)(ii)(C)	Access Establishment and Modification